

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA,)	
)	Case No. 17-cr-00134 (WMW-DTS)
)	
Plaintiff,)	DEFENDANT’S MEMORANDUM
)	IN SUPPORT OF MOTION TO
v.)	DISMISS INDICTMENT
)	BASED UPON AN
John Kelsey Gammell,)	UNCONSTITUTIONAL STATUTE
)	
Defendant.)	
)	

INTRODUCTION

Defendant John Kelsey Gammell submits this memorandum in support of his motion to dismiss the indictment. The government cannot establish the necessary nexus to interstate commerce. Moreover, the statute is vague. This Court should dismiss the indictment on constitutional grounds.

FACTUAL BACKGROUND

The Computer Fraud and Abuse Act (“CFAA”) enumerates federal crimes relating to the intentional access of certain computer without authorization or in excess of authorization. It also provides for civil remedies for violations. When Congress enacted the CFAA in 1984, the statute covered federal crimes primarily victimizing the government. 18 U.S.C. § 1030(a)(1)-(3) (Supp. II 1985) (criminalizing certain acts involving national security, financial records, and government property). The legislature has amended the statute five times in the decades since, creating confusion around the country as to the interpretation of its various provisions.

On June 5, 2017, the government charged Mr. Gammell in a one-count indictment alleging he “did knowingly cause and aid and abet the transmission ... and ... intentionally

caused damage, without authorization, to a protected computer.” Indictment at 1 [Docket 3]. In summary, the government alleges that from approximately July 2015 through September 2016, Mr. Gammell “caused or attempted to cause distributed denial of service attacks against targets” in Minnesota. *See* Criminal Compl. at 19-20 [Docket 1]. In particular, the government alleges Mr. Gammell targeted the website of the Washburn Computer Group (“Washburn”), a Monticello, Minnesota small business. *Id.* at ¶ 7. The government also contends that this conduct caused a loss of at least \$5,000 during one year.

LEGAL ARGUMENT

I. THE STATUTE EXCEEDS CONGRESSIONAL POWER UNDER THE INTERSTATE COMMERCE CLAUSE.

One fact should have given the government pause before charging Mr. Gammell with a DDOS attack: the elementary Washburn website which lies at the heart of this case was not an organ of interstate commerce. *See Rewis v. United States*, 401 U.S. 808, 812 (1971) (reversing conviction where government failed to show interstate element). As such, the government’s indictment against Mr. Gammell should be dismissed as a violation of the United States Constitution.

Federal jurisdiction under 18 U.S.C. § 1030(a)(5)(A) is predicated on interstate commerce. The relevant section of the statute reads as follows:

- (a) Whoever—
 - (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; shall be punished as provided in subsection (c) of this section.

More particularly, the definition of “protected computer” turns on the existence of the element of interstate commerce. The relevant definition of 18 U.S.C. § 1030 specifies:

(e) As used in this section—

(2) The term “protected computer” means a computer—

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

This case is the latest iteration of federal prosecutorial indiscretion the United States Supreme Court condemned in *United States v. Lopez*, 514 U.S. 549 (1995). The Constitution creates a federal government of enumerated powers. *Id.* at 551. The “States possess primary authority for defining and enforcing the criminal law.” *Id.* at 561 n.3. “The Constitution mandates this uncertainty by withholding from Congress a plenary police power that would authorize enactment of every type of legislation.” *Id.* at 566.

The Pew Research Center estimates that 84% of households within the United States own a computer. Indeed, 73% of those computers possess an Internet connection. *See* Lee Rainie, et al. and D’vera Cohn, *Census: Computer Ownership, Internet Connection Varies Widely Across U.S.*, (Sept. 19, 2014), <http://www.pewresearch.org/fact-tank/2014/09/19/census-computer-ownership-internet-connection-varies-widely-across-u-s/>. The Cellular Telecommunications Industry Association (CTIA) reports that wireless devices outnumber humans and places the number of active wireless devices at 396 million in a U.S. population of 327 million people. *See Americans’ Wireless Data Usage Continues to Skyrocket* (May 9, 2017), <https://www.ctia.org/industry-data/press-releases-details/press-releases/americans-wireless-data-usage-continues-to-skyrocket>. Nielsen’s estimates that 118.4 million households in the United States own at least one television. *See Nielsen Estimates 118.4 Million TV Homes In The U.S. For The 2016-17 TV Season* (Aug. 26, 2016),

<http://www.nielsen.com/us/en/insights/news/2016/nielsen-estimates-118-4-million-tv-homes-in-the-us--for-the-2016-17-season.html>.

Virtually every business uses multiple of these mechanisms to communicate. Indeed, virtually every American possesses numerous computers, phones, and other communication devices. But to federally criminalize any attempted attack on those electronic devices, however weak or unsuccessful, would be to assert “there would be virtually no limit to the federal power and for all practical purposes we should have a completely centralized government.” *Lopez*, 514 U.S. at 556. Allowing such limitless reach would cause every electronic device in the country to fall within the reach of the statute. This would violate well-established tenets established by the Supreme Court.

Were we to adopt the Government’s expansive interpretation of § 844(i), hardly a building in the land would fall outside the federal statute’s domain. Practically every building in our cities, towns, and rural areas is constructed with supplies that have moved in interstate commerce, served by utilities that have an interstate connection, financed or insured by enterprises that do business across state lines, or bears some other trace of interstate commerce If such connections sufficed to trigger § 844(i), the statute’s limiting language, “used in” any commerce-affecting activity, would have no office We conclude that § 844(i) is not soundly read to make virtually every arson in the country a federal offense.

Jones v. United States, 529 U.S. 848, 857-58 (2000) (declining to federalize all crimes of arson).

Congress possesses the power to regulate channels of interstate commerce, instrumentalities of interstate commerce, and activities having a substantial relation to interstate commerce. However:

Interstate commerce power must be considered in the light of our dual system of government and may not be extended so as to embrace effects upon interstate commerce so indirect and remote that to embrace them, in view of our complex society, would effectually obliterate the distinction between what is national and what is local and create a completely centralized government.

Lopez, 514 U.S. at 557.

The only Eighth Circuit case to ever address 18 U.S.C. § 1030(a)(5)(A)’s constitutionality demonstrates precisely why the government’s prosecution of Mr. Gammell is so inapt. In *United States v. Trotter*, 478 F.3d 918 (8th Cir. 2007), the appellate court rejected a constitutional challenge as applied to a defendant who allegedly attacked a global organization (the Salvation Army), deleted many of its files over the course of many days, shut down its phone system, and forced the Salvation Army to spend \$19,000 to repair the direct damage the defendant caused. *Id.* at 919-920. The defendant challenged the constitutionality of the statute claiming it did not cover a nonprofit organization such as the Salvation Army. *Id.* at 919. The court rejected the defendant’s challenge and ruled the Salvation Army’s nonprofit status was irrelevant.¹ *Id.* at 921.

By contrast here, the government alleges Mr. Gammell attacked a local company which experienced a grand total of three visitors in the months leading up to the alleged attack. *See* Ex. A at 00000536. A company official, encouraged by the FBI, ventured a guess as to \$3,000 to \$5,000 worth of damages, a guess nowhere quantified in the government’s vast files of discovery. *See* Ex. B at 00000463. Later, with the statutory minimum looming over the case, substantially inflated figures were produced asserting damages of \$40,000. Again, the government does not specifically delineate those numbers.

In enacting 18 U.S.C. § 1030, Congress intended to criminalize behavior with a “compelling federal interest.” *Prosecuting Computer Crimes Manual*, Office of Legal Education, Executive Office for U.S. Attorneys, U.S. Department of Justice (2010) (*citing* S.

¹ The *Lopez* argument was not a factor in the *Trotter* case because the defendant admitted as part of his plea agreement and guilty plea colloquy that the Salvation Army computers regularly used the internet to communicate with internal and external parties outside the state. *Id.* at 921.

Rep. No. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482). The Washburn Company is not a Fortune 100 company. At the time of the original alleged attack, it did not conduct commercial transactions over the Internet. It did not allow its customers to “sign in” to request information, bills, or services. It claims no lost business as a result of the cyber issue, nor could it. *See generally* Ex. C.² No evidence exists that these facts fulfill the statutory requirement that the web site was “used in” interstate commerce. *Cf. Jones*, 529 U.S. at 854 (“The proper inquiry, we agree, is into the function ... and then a determination of whether that function affects interstate commerce.”). Washburn’s very rudimentary web page is basically an advertisement for services, not a channel of interstate commerce.

This is a bit like claiming Mr. Gammell took down an “open for business” sign of a company which experienced no foot traffic, obtained no business through in person solicitations, and then installed a security camera to deal with such hijinks. At worse, the actions alleged in the indictment rise to the level of a prank, not a federal felony. The prosecution against Mr. Gammell, in failing to distinguish “between what is truly national and what is truly local,” exceeds the scope of Congressional power under the Commerce Clause. *See United States v. Morrison*, 529 U.S. 598, 617-18 (2000) (holding Commerce Clause did not empower Congress to enact broad criminal statute against gender violence affecting potentially half of nation).

This statute was enacted to punish criminals and crimes of significant import, *e.g.*, Dread Pirate Roberts, master of the cyber underworld. *See, e.g., United States v. Ulbricht*, 858 F.3d 71 (2d Cir. 2017). Of the very few times the U.S. Department of Justice has employed this particular statute, the defendants charged have engaged in conduct which allegedly

² Tellingly, the government does not even have (or apparently has not produced) evidence of what the web pages looked like on the days of the alleged attacks. The page’s appearance today is not evidence of what it may have looked like on the relevant dates.

commandeered the web sites of major commercial entities engaged in global commerce.³ The government's lack of real evidence on this matter, underscore further why this case is such a poor vehicle for federal prosecution. To put it plainly, John Kelsey Gammell is no Dread Pirate Roberts. Mr. Gammell respectfully requests the Court to dismiss the indictment for unconstitutionality as applied to Mr. Gammell.

II. THE STATUTE IS UNCONSTITUTIONALLY VAGUE IN VIOLATION OF MR. GAMMELL'S FIFTH AND FOURTEENTH AMENDMENT RIGHTS.

The statute is impermissibly vague, and the indictment should be dismissed under the Fifth and Fourteenth Amendments. *See Johnson v. United States*, 135 S. Ct. 2551, 2556 (2015) (reversing conviction under vague statute as violation of Fifth Amendment); *Collins v. Kentucky*, 234 U.S. 634 (1914) (reversing antitrust conviction under vague statute as violation of Fourteenth Amendment). The Fourteenth Amendment prohibits the government from denying "to any person within its jurisdiction the equal protection of the laws." U.S. CONST. amend. XIV, § 1. The Fifth Amendment guarantees criminal defendants due process under the law. U.S. CONST. amend. V. The statutory provision in this case requires a \$5,000 threshold "loss" for the punishment the government seeks to inflict on Mr. Gammell. *See* Indictment at 1 [Docket 3]. This portion of the statute carelessly defines "loss" in a manner that essentially allows the victim to determine the defendant's level of punishment, in contravention of the Constriction.

In interpreting a statute, a court will begin with the plain language of the statute. *See United States v. Staples*, 511 U.S. 600, 605 (1994) (reversing conviction where defendant claimed lack of awareness of properties which made firearm illegal). If the language is

³ Denial of service events are a common occurrence on the internet, "often occurring daily without any violent consequences." Paul A. Walker, *Rethinking Computer Network "Attack" Implications for Law and U.S. Doctrine*, 1 Nat'l L. Brief 33, 53 (2010) (quoting technical study finding an average of 2,000 to 3,000 active denial of service actions per week over three-year period).

unambiguous, the court's task is complete. *See United States v. Home Concrete & Supply, LLC*, 566 U.S. 478 (2012) (refusing to extend IRS limitations period in purported deficiency action against taxpayer). Any "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *United States v. Bass*, 404 U.S. 336 (1971) (reversing conviction for government's failure to prove interstate commerce nexus).

Criminal statutes must provide fair warning of federal crimes. *United States v. Powers*, 572 F.2d 146, 150 (8th Cir. 1978) (dismissing certain convictions obtained under ambiguous statute). The Congress, not prosecutors or courts, ought to define crimes. *Id.* at 150. A statute should be invalidated for vagueness if it fails "to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits" or it if "authorize[s] arbitrary and discriminatory enforcement." *City of Chicago v. Morales*, 527 U.S. 41 (1999) (invalidating for vagueness gang loitering ordinance). As Justice Holmes famously wrote:

It is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear.

McBoyle v. United States, 283 U.S. 25 (1931) (reversing conviction where defendant challenged vague statute and government's interpretation of crime).

Finally, the void for vagueness doctrine is a question of law. *See United States v. Hiland*, 909 F.2d 1114, 1142 (8th Cir. 1990) (refusing to allow government to assess to defendant costs of investigation).

Among its many amendments to the statute, Congress recently revised the statute to define "loss."

(11) The term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any

revenue lost, costs incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. § 1030 (e)(11).

The statutory definition presents more questions than answers and in no way provides a clear standard. Who decides what is a “reasonable cost to any victim”? Congress indicates it will be the victim. When is this “reasonable cost” established? Well after the crime, even up to a year, says Congress. *See* § 1030(c)(4)(A)(i)(I). What are “consequential damages”?⁴ On this, Congress is silent.

Mr. Gammell could not “knowingly” cause \$5,000 worth of damage when the victim in its sole subjective discretion defined the amount of loss years after Mr. Gammell allegedly committed the crime. *See Flores-Figueroa v. United States*, 556 U.S. 646 (2009) (“knowingly” modifies all clauses of criminal statute). Here, even the victim did not initially know with clarity how much loss Mr. Gammell allegedly caused. More disturbingly, the facts of this case show the government initially failed to meet the damages requirement and inflated its figures when it became clear it could not clear the threshold. *Cf.* Ex. B with Ex. D. The statute’s vague language invites this arbitrary enforcement.

Moreover, while considerations such as a damage assessment or purported consequential damages may be fair to consider in establishing restitution, it is a deprivation of Mr. Gammell’s due process rights to allow these factors, in the sole discretion of the victim, to determine his term of imprisonment by making the victim’s loss claim a jurisdictional element of the offense. *See Fields v. City of Omaha*, 810 F.2d 830 (8th Cir. 1987) (vague criminal statute failed to established fair standards and deprived defendant of due process).

⁴ The statute’s loss definition also conflates the civil and criminal law, which is particularly ironic since the statute itself allows victims to separately make claims for civil damages under similar principles. *See* 18 U.S.C. § 1030(g).

Disconcertingly, by the government's own claims, Mr. Gammell did not personally attack the Washburn web site. Instead, the government alleges Mr. Gammell hired "DDOS for hire services" to attack the web site. *See* Criminal Compl. at ¶¶ 3-4, 15-24, 28 [Docket 1]. The government has failed to charge a single one of those "cyber hit men" services, named and evidently well known to the government. If any person or entity impacted interstate commerce and has the potential to do so in the future, it is these unaccountable professional cyber hit men for hire. *See Kolender v. Lawson*, 461 U.S. 352 (1983) (invalidating statute which "encourages arbitrary enforcement"). Instead, the government's neglect has allowed the professional cyber hit men for hire to skip off merrily into the night.

Other courts already have criticized the CFAA as exceedingly vague, noted the strife it has sown between courts differently interpreting the same provisions, and invalidated portions of the statute. *See, e.g., United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (invalidating overly broad criminal component of 18 U.S.C. § 1030). *See generally*, Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596 (2003). With expansive interpretations, "behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever." *Nosal*, 676 F.3d at 862. That massive indeterminateness is precisely what the Constitution prohibits.

CONCLUSION

For the foregoing reasons, Mr. Gammell respectfully requests that the Court dismiss the indictment.

Dated: August 18, 2017

By s/Rachel K. Paulose

Rachel K. Paulose
DLA Piper LLP (US)
Attorney ID No. 0280902
80 South Eighth Street, Suite 2800
Minneapolis, Minnesota 55402-2013
Telephone: 612.524.3008
Facsimile: 612.524.3001
rachel.paulose@dlapiper.com

ATTORNEY FOR DEFENDANT

EAST\145072323.1